Environmental Sustainability in the Arctic

On Modern Threats to Environmental Sustainability in the Arctic: The Cybersecurity Factor and the Provisions of Insurance Against Environmental and Cyber Risks in Oil and Gas Installations

*Kyriaki Noussia**

Due to unprecedented fires and rise in temperature climate change is occurring rapidly, melting the Arctic ice and uncovering new areas for expropriation of natural resources. Such expropriation needs to occur in a sustainable way, respecting the environment and the indigenous people. To achieve this, all inherent risks arising from any environmental threat (oil spill/any type of environmental accident, cyber risks of any nature) to oil and gas installations need be identified and environmental liability and cyber-risks insurance coverage need be in place. This article discusses the way for such insurance coverage to be placed and worded. It argues that the traditional (marine and other) property insurance policies coverage and wording is inefficient, as it ends up being fragmented due to the numerous policy exclusions and limitations; it also puts forward an argument for the need to have specific wording and cover for specialized risks, in relation to the operation of oil and gas installations in the Arctic and cyber-risk threats, taking into account potential environmental impacts and hazards. This article also argues that for the time being, as businesses and governments including those of the EU and the Member States become increasingly reliant on technology, it is imperative that additional cyber-related risks are identified and minimized or transferred externally. Finally, it offers some suggestions about cybersecurity policies covering specialized risks.

Keywords: *Sustainability, Arctic, Cybersecurity, Environmental pollution, Environmental pollution liability, Offshore oil and gas*

1 Introduction

In the Arctic, as the climate change pace accelerates, new geographical areas, most of which are off-shore, will emerge, with the potential of expropriation of natural resources. Alongside these newly emerging exploitable areas, will also arise the need to expropriate in a sustainable manner and to provide adequate mitigating measures, in order to address potential environmental harm or pollution.[1]

The globalization of environmental risk poses a mounting challenge to policy makers, not least because it now entails the cyber-risk relating to malicious cyber-attacks on oil and gas off-shore installations. As of yet, the rules of responsibility for harm production remain underdeveloped, in spite of the negotiation and implementation of numerous international environmental agreements.[2] The civil liability regime for marine and oil pollution was the first to broaden compensation obligations beyond personal injury and property damage to include environmental impairment and has paved the way for the liability rule for all oil and gas expropriation activities.[3] Several types of insurance might respond to pay for losses stemming from an oil spill, including, insurance policies for first-party property, 'business interruption' and 'loss of production income' insurance, 'directors & officers liability' (D&O) insurance, 'event cancellation' insurance, 'trade disruption' insurance, 'environmental liability' insurance, marine insurance, 'comprehensive general liability' (CGL) insurance, insurance for operator's extra expenses – occurred for the control of the well, physical damage insurance, workers compensation or employers liability insurance, as well as cyber insurance for risks related to malicious cyber-attacks on the infrastructure of oil and gas installations, which can lead to multiple types of losses and damages, including environmental oil pollution.[4]

Cyber-insurance has a broad definition and although it was originally defined as insurance for the damages to 'physical' computer equipment, nowadays it represents a risk mitigation tool for IT/cyber-related losses, covering damages or losses from information/IT systems and networks. It is suggested[5] that cyber-insurance promotes the implementation of good security measures. However,

* Senior Lecturer in Law, University of Exeter, Law School, CSSIS, Amory Building, Rennes Drive, EX4 4RJ, UK
Email: k.noussia@exeter.ac.uk.

[1] K. Noussia, *The BP Oil Spill – Environmental Pollution Liability and Other Legal Ramifications*, 3 E. E. E. L. R. 98–107 (2011).

[2] *Ibid.*

[3] K. Mason, *Transnational Compensation for Oil Pollution Damage: Examining Changing Spatialities of Environmental Liability*, LSE Research Papers in Environmental and Spatial Analysis (RPESA), no. 69, 1–24 at 1–3 (Department of Geography and Environment, LSE, London 2002); B. Sandvik & S. Suikkari, *Harm and Reparation in International Treaty Regimes: An Overview*, in *Harm to the Environment: The Right to Compensation and the Assessment of Damages*, 57–71 at 64–65 (P. Wetterstein ed., Clarendon Press, Oxford 1997).

[4] Noussia, *supra* n. 1, at 98–107; Mason, *supra* n. 3, at 1–24, 1–3; Sandvik & Suikkari, *supra* n. 3, at 57–71, 64–65.

[5] R. Anderson et al., *Security Cconomics and the Internal Market* (Heraklion: ENISA 2007), https://www.enisa.europa.eu/publications/archive/economics-sec/ (accessed 3 Mar. 2020).

innovations in the cyberspace introduce new types of losses and act as barriers to effective coverage. In addition, the Internet of Things (IoT) is shifting cybersecurity from protecting information assets to physical goods previously unrelated to computers.[6] At present, cyber insurance does not dominate the overall non-life insurance market,[7] but it is one of the fastest-growing new lines of insurance business and cybersecurity is recognized as one of the top global risks.[8] Meanwhile, more and more traditional insurance contracts exclude specific losses linked to cybersecurity, and therefore, it is imperative that a separate cyber-insurance market develops, in an effort to also assist industry practitioners and regulators to fully understand potential future systemic risks.[9]

The (offshore) energy insurance market is highly specialized and because the limits of insurance are usually in the excess of USD 1 billion, there is no single insurer who covers the entire risk exposure. Oil and gas firms, whether they have experienced cyber-attacks or not, are incentivized to assure that their business processes are resilient, in the face of cyber-events, internally and externally, to comprehend the impact of systemic risk to cyber-events, and be responsive and resilient in addressing such emerging risks and protecting critical oil and gas installations and other infrastructure. Because we live in an era where there is an increased use of the IoT across the energy sector, this also increases the vulnerability to cyber-attacks. Therefore, it is imperative to address cyber-risk as a key operational risk and implement measures to prevent, detect and respond to cyber-threats in a holistic way. In addition, the provision of more detailed information from the energy industry and the cooperation with underwriters, will help the insurance industry improve its coverage of energy assets and to further develop cyber-insurance products. The insurance as a mitigating measure and option apart, businesses with operational technology networks (OT), including oil and gas expropriation installations need to be in a position to implement mitigating measures so as to understand cyber risks and be able to assess, identify and rectify cybersecurity vulnerabilities and also prevent attacks that exploit these vulnerabilities.[10] Such mitigating measures, together with cyber-insurance will help offset the potential financial impacts of a cyber-attack.[11]

2 The case of 'Deepwater Horizon' and the 'Saudi Aramco' 2012 & 2019 Incidents: The Need for Response to Cyber and Environmentally Impaired Incidents

On 20 April 2010, the Deepwater Horizon (DWH), a semi-submersible mobile offshore drilling rig owned and operated by Transocean Ltd., caught fire and sank in the Gulf of Mexico, off the shores of Louisiana. The rig was drilling a prospect known as 'Macondo', some fifty miles off the coast of Louisiana, in 5,000 feet of water. British Petroleum (BP) Plc – along with its partners Anadarko Petroleum Corp. and Mitsui Oil Exploration Co. – acquired the prospect in 2008 in a sale of leases run by the USA government's Minerals Management Services. The well had been drilled to 18,000 feet when a blow-out occurred. The explosion, and fire that followed, killed eleven out of the 126-man crew. A day and a half later the rig collapsed into the sea and sunk, and oil begun to spread across the surface of the water, eventually making landfall to the north-east.[12] BP, being the majority stakeholder in 'Macondo' was largely identified with the spill. Anadarko Petroleum Corp. and Mitsui Oil Exploration Co. owned 25% and 10% stakes in the well, respectively, and hence also a share in the cost of responding to the oil spill. The oil platform was being leased by Transocean Ltd. to BP Plc., and following the accident sat on the sea floor over 5,000 feet below sea level. Prior to the explosion on 20 April 2010, Halliburton Co. had been engaged in cementing operations on the well, and cementing operations had previously been associated with other oil-well accidents.[13] The amount of oil and gas, escaping from the subsurface well had been estimated to have been in the range of 35,000–60,000 barrels of oil a day, making the incident the largest oil spill in USA history.[14] The 'Macondo' oil-

[6] Anderson et al., *supra* n. 5; P. Petratos, A. Sandberg & F. Zhou, *Cyber insurance*, in *Handbook of Cyber-Development, Cyber-Democracy, and Cyber-Defence* 809–836, 809–810 (E. Carayannis, D. Campbell & M. P. Efthymiopoulos eds, Springer 2017)

[7] Marsh, *UK Cyber Security: The Role of Insurance in Managing and Mitigating the Risk: Technical Report* (UK HM Government 2015), https://www.marsh.com/uk/insights/research/uk-cyber-security-role-of-insurance-in-managing-mitigating-risk.html (accessed 3 Mar. 2020).

[8] WEF, *Global Risks 2015, Technical Report*, (World Economic Forum, Geneva 2015), http://www3.weforum.org/docs/WEF_Global_Risks_2015_Report15.pdf (accessed 3 Mar. 2020).

[9] Anderson et al., *supra* n. 5; Petratos, Sandberg & Zhou, *supra* n. 6, 809–836 at 809–810; Marsh, *supra* n. 7.

[10] PricewaterhouseCoopers, *Cyber Savvy: Securing Operational Technology Assets*, (Canada 2016), https://www.pwc.com/ca/en/consulting/publications/2016-01-18-pwc-cyber-savvy-securing-operational-technology-assets.pdf (accessed 3 Mar. 2020).

[11] World Energy Council, *World Energy Perspectives: The Road to Resilience: Managing Cyber Risk* (2016), https://www.worldenergy.org (accessed 3 Mar. 2020).

[12] Focus, *Macondo*: *Assessing the Implications*, 35(7) Oil & Energy Trends 3–6, at 3 (2010)

[13] Michael Kotula, Insurance and the Gulf of Mexico Oil Spill, LexisNexis Legal Room, Insurance Law, (2010), https://www.lexisnexis.com/legalnewsroom/insurance/b/insurance-law-blog/posts/insurance-and-the-gulf-of-mexico-oil-spill (accessed 3 Mar. 2020).

[14] Focus, *supra* n. 12, 3–6 at 3; Kotula, *supra* n. 13; King, *supra* n. 13, at 3; Deepwater Horizon Unified Command, *U.S. Scientific Team Draws on New Data, Multiple Scientific Methodologies to Reach Updated Estimate of Oil Flows from BP's Well* (15 June 2010), http://www.deepwaterhorizonresponse.com/go/doc/2931/661583 (accessed 3 Mar. 2020); A. Winter, *USGS Director Quietly Wages Fearless War on Oil Spill*, New York Times

Environmental Sustainability in the Arctic

well, was initially sealed in mid July 2010, eighty-seven days after the incident occurred, it was then subsequently further sealed in early August 2010, having reached the amount of four, one million oil barrels, and finally cemented on 19 September 2010.

In 2012, the oil and gas world witnessed the worst hack ever seen to that date. A monstrous cyber-attack on Saudi Aramco, one of the world's largest oil companies, almost halted the world's oil production and almost created a worldwide economic crash. The incident entailed one of the computer technicians on Saudi Aramco's information technology team opening a scam email and innocently clicking on a bad link, hence without knowing it, allowing the hackers in. The incident of the cyber-attack occurred in August 2012 during the Islamic holy month of Ramadan, when most Saudi Aramco employees were on holiday. Initially, some employees noticed their computers were having problems in operating. In a matter of hours, 35.000 computers were partially wiped or totally destroyed, as a result of which operations were halted and Saudi Aramco's ability to supply 10% of the world's oil was suddenly at risk. Oil production remained steady but managing supplies, shipping, contracts with governments and business partners, was forced to happen on paper and the company was suddenly forced to be propelled back into 1970s technology, using typewriters and faxes. As a result, the company temporarily stopped selling oil to domestic gas tank trucks and later on, after seventeen days, the corporation relented and started giving oil away for free to keep it flowing within Saudi Arabia. A massive army of IT people were hired as independent consultants to help secure all of Saudi Aramco's satellite offices in Africa, Europe and the Middle East. Aramco's representatives were flown directly to computer factory floors in Southeast Asia to purchase every computer hard drive currently on the manufacturing line. This caused a temporary worldwide shortage on hard drives, as Aramco bought in one instance 50,000 drives. Five months later, with a newly secured computer network and an expanded cybersecurity team, Saudi Aramco brought its system back online. However, the repercussion and ramifications were still to be felt for many months to follow thereafter. It is a blessing in disguise that no connection to networks was possible for storage tanks at that time. The attack was a wake-up call for the possible ramifications of a possible further cyber-attack in the oil and gas sector.[15]

In September 2019, drone attacks at two Saudi Aramco oil facilities forced the shut-down of half its total oil production. The strikes targeted Saudi Arabia's Abqaiq and Khurais oil facilities, sparking concern about global oil supply stability, which severely disrupted global energy infrastructure and sent crude prices soaring by double digits. Abqaiq, located in the kingdom's oil-rich Eastern province, is the world's largest oil processing facility and crude oil stabilization plant with a processing capacity of more than seven million barrels per day (bpd). Khurais, which lies about 110 miles southwest of Abqaiq, has capacity to pump around 1.5 million bpd.[16]

Following the attacks, Saudi Aramco was looking to buy insurance against war and terror attacks after a damaging drone and missile attack on some of its oil facilities in September 2019. Aramco had not insured against all risks and its cover did not protect it from terrorism or acts of war. Available additional insurance options would range from cover against a terror attack or sabotage through to full coverage, which includes war or civil war, along with compensation for the cost of business interruption.[17] In addition cyber-risk insurance coverage was sought to be added on any additional war risk coverage, to enhance recovery available options.

Not only the DWH which was owed to a mechanical failure, but also the Saudi Aramco cyber-attack in 2012 forced for a response in the regulatory landscape for environmental pollution liability and triggered changes in the insurance industry landscape regarding environmental and cyber-related risk coverage. However, the response from the insurance industry has not been the one anticipated and the insurance industry itself has been criticized as failing to keep up with changes in the legal and regulatory environment post these events.[18]

Due to the fact that oil pollution damage can occur as a result of an off-shore oil expropriation incident or due to cyber-security attacks in oil and gas companies' headquarters, as the DWH and Saudi Aramco incident have revealed, oil spill related costs can accrue and make it extremely difficult for companies to draw a line, as not only is it difficult to anticipate the actual losses occurred during oil pollution and other general or cyber-related liability incidents, but to also place caps in such liabilities. Post these incidents, insurers have tended to add crisis management services to their environmental insurance solutions. Regulators have also appeared as stepping up their enforcement of environmental and other laws. In addition, it was realized that there is a lack of uptake of financial security instruments to cover all damage from the most infrequent and costly offshore accidents.[19]

(16 June 2010), http://www.nytimes.com/gwire/2010/06/16/16greenwire-usgs-director-quietly-wages-fearless-war-on-oi-83792.html (accessed 3 Mar. 2020).

[15] J. Pagliery, *The Inside Story of the Biggest Hack in History*, CNN Business (8 May 2015), https://money.cnn.com/2015/08/05/technology/aramco-hack/index.html (accessed 3 Mar. 2020).

[16] D. Reid, *Saudi Aramco Reveals Attack Damage at Oil Production Plants*, CNBC (21 Sept. 2019), https://www.cnbc.com/2019/09/20/oil-drone-attack-damage-revealed-at-saudi-aramco-facility.html (accessed 3 Mar. 2020).

[17] M. Safi & G. Waerden, *Everything You Need to Know About the Saudi Arabia Oil Attacks*, The Guardian (16 Sept. 2019), https://www.theguardian.com/world/2019/sep/16/saudi-arabia-oil-attacks-everything-you-need-to-know (accessed 3 Mar. 2020).

[18] Pagliery, *supra* n. 15; CIR, *Lloyd's: Offshore Energy Underwriting 'Out of Step'* (22 Sept. 2011), http://www.cirmagazine.com/cir/lloyds-offshore-energy-underwriting-out-of-step.php (accessed 3 Mar. 2020); Insurance Insight, *Bolt Criticises Energy Underwriters* (22 Sept. 2011).

[19] PricewaterhouseCoopers, *supra* n. 10.

Environmental Sustainability in the Arctic

Therefore, extensive and responsive mitigating measures would have to have been in place alongside extensive insurance cover for cyber-attack risks. This has even more been reiterated following the September 2019 drone attacks on Abqaiq, Saudi Aramco's crude processing centre, and in the Khurais oilfield. The latest drone attack has forced the company to work harder so as to implement measures that would allow it to mitigate against an equally possible risk of cyber-attacks. Saudi Aramco has since been working intensively to secure their infrastructure, as they recognize it now as a constant threat.

Possible recommendations for future steps could include the introduction and collection of data on damages resulting from such incidents to help better address insurance coverage needs, or the creation of an international organization to monitor safety standards and establish an international safety standard as a safety goal for all drilling industries to meet, which, would act as a mitigating measure in implementation and, in this way, would also help streamline the insurance coverage offered and establish a stable 'soft' insurance market.

In addition, because a cyber-attack on an operational technology environment can have serious and wide ranging consequences beyond just financial losses, including prolonged outages of critical services, environmental damage and even the loss of human life, it is imperative that major operators not only take out additional insurance coverage but also assert stable mitigating measures and increase focus and spending also on their operational technology systems, which will enable them to identify and respond to cyber-security vulnerabilities.[20]

Sutherland argues that potential environmental exposures for energy companies entail large-scale catastrophic events with a considerable scale of potential losses. Post the DWH and Saudi Aramco incident, the London market had casualty offerings for the energy market such as follow-form excess liability limits available up to USD 50mn, or catastrophic, high excess limits available for up to USD 150mn. Such coverage was offered as an endorsement to the general casualty policy, for pollution events or through the guise of environmental impairment liability insurance (EIL) so as to be able to also cover regulatory obligations.[21]

Faure, Philipsen and Wang argue that possible recommendations for future steps, could include the introduction and collection of data on incidents related to damages resulting from (off-shore) oil and gas activities, or an international agreement for offshore-related incidents which would have to include a wide legal regime of strict liability for damage caused by offshore-related risks, establish a system of joint and several liability for the various parties involved in the offshore-related risk, and avoid financial caps on liability, in an effort to fully expose those involved in the offshore-related risks to the social costs of their activity and establish a mechanism able to facilitate early compensation payments to specific vulnerable groups of victims negatively affected by offshore- related incidents.[22]

3 The Environmental Pollution Insurance Landscape

3.1 Evolution and characteristic features of environmental insurance

In the early 1940s, property and casualty insurers started offering CGL insurance, which covered liability arising out of accidental or unexpected and unintended property damage or bodily injury that happened during the policy period, even if a claim was not made until long after the policy period.[23]

From the early 1970s, property and casualty insurers began to include the 'qualified' pollution exclusion in their policies, which excluded bodily injury or property damage unless sudden and accidental.[24] Around 1986, insurers began including the 'absolute' pollution exclusion in CGL policies, which excluded coverage for pollution claims whether or not they were sudden and accidental.[25] By the mid-1980s, insurers either stopped offering EIL coverage, or policyholders stopped buying EIL coverage, either because it had become prohibitively expensive or due to the fact that claim expenses had outpaced premium revenues. However, by the late 1990s, new environmental insurance products began to appear such as 'Pollution Legal Liability Insurance', 'Clean- up Cost Cap Insurance', or a number of more specialized products, such as 'Contractors Pollution Liability Insurance', 'Commercial Real Estate Pollution Legal Liability Insurance', and 'Contaminated Property Development Insurance'.

Plumer, Lathrop, Suomela and Waeger, all state that different coverages may apply to pollution that begins before the policy period as compared to pollution that begins during the policy period. Additionally, some policies only cover 'sudden' pollution events (i.e. 'abrupt'), and some policies may require that the pollution be discovered within a defined period of time (e.g. within an X amount of hours post the occurring event), or they may have very short reporting periods (e.g. thirty days) in order for coverage to apply, coupled with the fact that different coverages are required to address potential on-site clean-up versus other third-party liability.[26]

[20] *Ibid.*
[21] S. Sutherland , *Paying for Pollution*?, AIG Environmental Insurance, AIG – Insider Quarterly's, 2015, Winter Issue https://www-409.aig.co.uk/content/dam/aig/emea/united-kingdom/documents/Insights/aig-iq-winter-2015-eil-article.pdf (accessed 15 Mar. 2020).
[22] M. Faure, N. Philipsen & H. Wang, *Concluding Remarks*, in *Civil Liability and Financial Security for Offshore Oil and Gas Activities* 383–387 (M. Faure ed., 2016).
[23] M. Plumer, A. Lathrop & K. Suomela, *Insurance for Environmental Claims*, New Appleman on Insurance 33–39 at 33–34 (2010).
[24] For example, ISO 1973 Standard Form for CGL Policy.
[25] Plumer, Lathrop & Suomela, *supra* n. 23, 33–39 at 33–34.
[26] A. Waeger, *Current Insurance Policies for Insuring Against Environmental Risks* in *Environmental Insurance: Emerging*

Environmental Sustainability in the Arctic

Merkin rightly emphasizes the fact that because 'sudden' and 'unexpected' loss coverage is usually found in property casualty policies, it follows that it does not quite fit the case of environmental pollution, because environmental pollution as such is usually gradual. Hence, it is argued that there is some ambiguity as to what 'sudden' actually means, in the context of EIL policies. The real question that arises here is at which stage is 'sudden' established in terms of coverage purposes. Property policies generally require a loss from one or more specified perils to arise from an accidental, sudden or unforeseen event or occurrence.[27]

The word 'accidental', means that the loss suffered by the assured has be an 'unlooked-for mishap or an untoward event which is not expected or designed.'[28] The mere fact that the insured subject matter has sustained damage is, therefore, not sufficient to trigger coverage under a property policy. By way of example, if the subject matter disintegrates[29] or collapses and the assured cannot show that there has been an accidental event triggering the damage, then there is no recovery.[30] In *Pacific Chemicals Pte Ltd v. MSIG Insurance (Singapore) Pte Ltd*[31] it was held that the phrase 'any unforeseen and sudden physical loss destruction or damage' meant that the damage had to be sudden and accidental, so that it was irrelevant that the peril which had caused the damage itself occurred slowly.[32]

In relation to clean-up costs, because such costs are not included in the coverage of property liability policies, the need for EIL policies arose, in order to have such cover also provided. Clean-up costs are not to be considered as falling into the category of damages, hence the definition[33] which is usually to be found in CLG policies is a rather limiting one. The term 'liability at law by way of damages' and equivalent wording has been held to not encompass compensation payable under a statutory obligation which imposes liability irrespective of the fault of the assured.[34]

In relation to marine policies, it is not compulsory in law to have environmental pollution liability coverage, however it is established in practice that an obligation exists by contract to have EIL insurance in place. It is also worth mentioning that usually EIL policies are reinsured in the London market, under English law. It follows from the above that the reinsured will have an obligation to hand over the conduct of settlement to reinsurers and get their prior consent.

3.2 Marine insurance coverage and claims in relation to an oil spill in the Arctic

Shipowners are free to assume the risk of trading and navigating on Arctic routes subject to obtaining suitable marine insurance, however the norm in the marine insurance market is to exclude or limit the coverage of Arctic marine perils through the imposition of navigating limitations for vessels as the passage in Arctic waters entails high risks.

Marine insurance in the Arctic is disadvantaged due to limited knowledge and information which results in insurers not being able to identify and assess the risks likely to be encountered in the various shipping routes. This uncertainty in defining and assessing the risks as well as the lack of reliable data results in increased deductibles for ice-related damages and in the consideration of Arctic related risks by insurers on a case by case basis. Although the international insurance market is prepared to underwrite shipping risks in the three Arctic corridors, i.e. The Northeast Passage (NEP), the Nothwest Passage (NWP) and the Transpolar Passage (TPP), however, the premiums charged will be different with the ones for the NWP and TPP being certainly higher than these for the NEP on the basis of the variously differentiated risk factors that exist in the various passages.

With regards to navigating limits, although the Institute Time Clauses do not refer to them, this is done via the reference to the Institute Warranties which exclude perils of the seas in certain areas and contain a list of warranties relating to geographical limits of navigation. 'Held covered' clauses also allow the assured shipowner to cover marine risks and to avoid the consequence of no insurance liability and coverage in the case that the navigating limits are breached.[35] Entry is allowed into the Arctic only

Issues and Latest Developments on the New Coverage and Insurance Cost Recover, 339–472, 342–343 (ALI-ABA Course of Study Boston 8–9 May 2008), https://www.ali-cle.org/doc/frontmatter/CN050_fm.pdf (accessed 3 Mar. 2020); Plumer, Lathrop & Suomela, *supra* n. 23, 33–39 at 33–34.

[27] *Axa Reinsurance (UK) Plc v. Field* [1996] 3 All E.R. 517; *Marketform Managing Agency Ltd v. Amashaw Pty Ltd* [2018] NSWCA 70.

[28] Of the many authorities on 'accident', *see* e.g. *Fenton v. Thorley* [1903] A.C. 443; *Patrick v. Royal London Mutual Insurance Society Ltd* [2006] EWCA Civ 421; *C A Blackwell (Contractors) Ltd v. Gerling Allegemeine Verischerungs AG* [2007] EWHC 94 (Comm); *Sheehan v. Lloyds Names Munich Re Syndicate Ltd* [2017] FCA 1340.

[29] *Weir Services Australia Pty Ltd v. AXA Corporate Solutions Assurance* [2018] NSWCA 100, concerned a liability policy, but the same principles are applicable - there the Court was able to point to a fortuity.

[30] *Leeds Beckett University v. Travelers Insurance Company Ltd* [2017] EWHC 558 (TCC).

[31] *Pacific Chemicals Pte Ltd v. MSIG Insurance (Singapore) Pte Ltd* [2012] S.G.H.C. 198; *see also Australia Paper Manufacturers Ltd v. American International Underwriters* [1994] 1 V.R. 685.

[32] *See also Vee H Aviation Pty Ltd v. Australian Underwriting Pool Pty Ltd* unreported Dec. 1996, (ACT); R. Merkin, *Colinvaux's Law of Insurance*, (11th ed., London: Sweet & Maxwell, 2016), para. 20–055.

[33] Historically CGL policies would typically promise to provide coverage for all sums which the insured shall become legally obligated to pay as damages because of property damage to which this insurance applies, caused by an occurrence.

[34] *Tatham, Bromage & Co v. Burr (The Engineer)* [1898] A.C. 382; *Hall Brothers Steamship Co Ltd v. Young* [1939] 1 K.B. 748.

[35] P. K. Mukherje & H. Liu, *Legal Regime of Marine Insurance in Arctic Shipping: Safety and Environmental Implications*, in Sustainable Shipping in a Changing Arctic WMU Studies on

where permission has been obtained from the underwriter and where the requisite additional premium is agreed.

Seaworthiness is a cornerstone element in marine insurance contracts in that it is an implied warranty as per section 39 of the Marine Insurance Act (MIA) 1906. The ship needs be seaworthy, i.e. reasonably fit in all respects to encounter the ordinary perils of the sea at any stage of the maritime adventure, and the insurer is not liable if the assured sends the ship to sea in an unseaworthy state. Sea ice may be considered an ordinary peril if it exists in the normal course of a voyage in the Arctic. It will not be considered an ordinary peril if it exists only in certain 'ice-manifested' waters posing extraordinary and unpredictable navigational hazards. However, if a vessel is equipped for ice navigation in accordance with the Polar Code, then for its purposes the presence of ice could be an ordinary peril in that context. Hence, it follows that any vessel entering Arctic waters and non-complying with the Polar Code constitutes an unseaworthy vessel if such non-compliance leads to the vessel being non-fit in all respects for its intended purpose to navigate in the Arctic waters. Failure also to comply with the Polar Code is an emanation of breach of the seaworthiness requirement, for, the objective of the Polar Code is to ensure, inter alia, ship safety in Polar waters including the Arctic.[36]

Due to the fragility of the Arctic environment, P&I insurance covers third party liability of the shipowner for pollution damage causing harm to the marine environment. Again navigation limits play the role of promissory warranties which – if breached – will relieve the P&I Club from all liability as per the provisions of the MIA 1906. Mandatory insurance in the form of P&I cover is required for the potential liability of the shipowner for ship-source pollution damage in relation to Arctic shipping. In the case of the Arctic waters the P&I clubs face payment of indemnification associated with enhanced risks due to the presence of ice which has the potential for engendering casualties including collisions and groundings and consequential pollution in an environment that is ecologically fragile and where the pollutant does not really dissipate. The role of the P&I Club is crucial to the indemnification of pollution damage.[37]

In addition to the several types of insurance available to respond to pay for losses stemming from oil spills, in addition, insurance may be provided for mitigation costs.[38] However, in the domestic London market it has already proved necessary to adopt specific policies for environmental issues, so as to provide insurance for mitigation and remediation costs as well as to deal with the problem that policies traditionally cover only sudden fortuities rather than gradual environmental damage. Because the extent of property damage during an oil spill is often unclear, in many cases the coverage sought is the one provided for under an 'all-risk' policy whereby once a policyholder shows that it has suffered a loss, the burden of proof shifts to the insurer to show that the loss is not covered. Equally, a 'named peril' policy might be opted for, although it would only provide coverage for perils expressly listed. Both types of policies may contain exclusions to coverage. The likely claims to arise involve usually issues related to the basic elements of first-party coverage, i.e. (1) issues relating to covered property, (2) issues relating to the existence of a sustained physical loss or damage, and (3) the fact that there has to be a claim resulting from a covered peril.

Physical loss or damage has been defined in case law as well, such as in *Columbiaknit, Inc. v. Affiliated FM Insurance Co.*,[39] and in *Trinity Industries, Inc. v. Insurance Co. of North America.*[40] In the case of the BP oil spill, claims against BP Plc. offered a unique intersection of environmental, tort, administrative, maritime, and insurance law.[41]

3.3 Modern environmental coverage policies and arising disputes

The case law, regarding disputes under modern environmental policies, is not that vast as one would perhaps expect. The litigated issue under modern pollution coverage has mainly been the issue of whether the particular claim is one the specific pollution policy was intended to cover.[42]

In *Alan Corp. v. International Surplus Lines Ins. Co.*,[43] the insurer, International Surplus Lines Insurance Corporation (ISLIC), issued a pollution liability policy covering third party claims for property damage or bodily injury arising out of a pollution incident if the pollution incident and the third-party claim both occurred during the policy period. The policy covered 'reasonable and necessary clean-up costs incurred by the insured in the discharge of a legal obligation validly imposed through governmental action which is initiated during the policy period'. ISLIC denied coverage for Alan Corp.'s clean-up costs because, although the pollution incident occurred during the policy period, the governmental action was

Maritime Affairs, 191–225, at 202–205 (L. Hildebrand, L. Brigham & T. Johansson eds, Springer 2018).

[36] Mukherje & Liu, *supra* n. 35, 191–225, at 208–209.

[37] Mukherje & Liu, *supra* n. 35, at 215, 217, 219.

[38] For example companies may purchase equipment, such as booms, in an effort to protect property from contamination; L. Kellner et al., *Insurance Coverage Issues for Third-Party Businesses and Municipalities with Losses Due to the Oil Rig Explosion in the Gulf of Mexico* (Insurance Coverage Alert, Dickstein Shapiro LLP May 2010).

[39] *Columbiaknit, Inc. v. Affiliated FM Insurance Co.*, 1999 US Dist. LEXIS 11873 at 9 (D. Or. 1999).

[40] *Trinity Industries, Inc. v. Insurance Co. of North America*, 916 F.2d 267, 270–71 (5th Cir. 1990).

[41] W. C. Merlin Jr., *Understanding the Valuation Issues*, in *Conference Oil in the Gulf – Litigation and Insurance Coverage*, 1 (HB Litigation Conferences Atlanta; USA 2010).

[42] Plumer, Lathrop & Suomela, *supra* n. 21, 33–39 at 33–34.

[43] *Alan Corp. v. International Surplus Lines Ins. Co.*, 823 F. Supp. 33 (D. Mass. 1993); Plumer, Lathrop & Suomela, *supra* n. 21, 33–39 at 33–34.

Environmental Sustainability in the Arctic

not initiated until after the policy period. The court upheld ISLIC's denial of coverage.[44]

D.C. Operating Co., Limited Liability Company (LLC) v. Indian Harbor Insurance Co,[45] highlighted the often cited issue with regards to claims made under modern pollution coverage, whereby the fact that policyholders purchase pollution coverage as a result of an existing detection of contamination and so as to contemplate for potentially additional undetected contamination, does not guarantee that there will be no exclusion of the entire risk.

In addition, the practice of 'post-claim underwriting' by insurers may result in the insurer establishing that the assured did not disclose important information and hence avoid coverage, as was the case in *John R. McKenzie Jobber, Inc. v. Mid-Continent Casualty Co*[46] and as was further illustrated in *Viacom International, Inc. v. Admiral Ins. Co.,*[47] which allow us to conclude that policyholders may trigger current and historical CGL policies to cover the same claims, but their availability will largely depend upon the applicable policy language, (e.g. 'other insurance' provisions). Indeed, in *Viacom International, Inc. v. Admiral Ins. Co.*,[48] the court interpreted a somewhat unusual 'other insurance' provision in the EIL policies, which allowed the policyholder to treat the EIL coverage as either primary or excess to other applicable insurance.[49]

4 Specific Insurance Issues Raised in Case of a Major Oil Spill

Accidents such as the DWH oil spill raise certain insurance issues. Such issues pertain inter alia to the insurability of the incident *per se* as well as of the kind of damages sustained, on the environmental side, and to the question of whether such liability should be capped or not. In relation to the specific insurance issues raised by the DWH accident, and more specifically in relation to the actual insurability of the damages sustained, due to the fact that most EIL policies are reinsured in the London market, it is essential to assess insurability under the scope of reinsurance case law.

Prior to the decision of the House of Lords in *Wasa International Insurance Co Ltd v. Lexington Insurance Co*,[50] the nature of the reinsured's insurable interest was debatable, i.e. one view pertained that the reinsured's insurable interest exists in its liability, which renders a reinsurance agreement something akin to a liability policy,[51] whereas the alternative view was that reinsurance is 'the insurance of an insurable interest in the subject matter of an original insurance',[52] however the point had been left open in a number of cases.[53] In *Wasa International Insurance Co Ltd v. Lexington Insurance Co*,[54] the House of Lords took the view that reinsurance was not liability insurance at all, but constituted a further insurance on the original subject matter, although it was accepted that there was much to be said for the liability insurance argument and that it was open to the parties to frame their contact as one on liability.[55]

Following a major off-shore accident various mechanisms, i.e. financial and insurance instruments, are used to cover liability risks and as such often cover both first-party damage, including well-control, and liability. One way to provide adequate coverage is via self-insurance which serves as a mechanism whereby larger players in the market run the risk themselves, a) either via issuing pure self-insurance which in essence acts as a reserve for potential losses and whereby operators use their balance sheet to guarantee payment in case of a major accident occurring, or b) via a captive which would be created by a major offshore operator and would function de facto as an insurance company, however with no loss spreading.

Existing insurance coverage for off-shore activities mainly covers physical damage and liability exposures. The risks may involve construction, physical damage, removal of wreckage, control of the well, and liability. The policies involved include 'off-shore physical damage coverage' for all risks associated with physical loss or

[44] *Ibid.*
[45] *D.C. Operating Co., LLC v. Indian Harbor Insurance Co*, decision and order granting in part and denying in part the defendants' motion to dismiss the complaint, No. 07-CV-0116 (S.D.N.Y. 27 Mar. 2007).
[46] *John R. McKenzie Jobber, Inc. v. Mid-Continent Casualty Co.*, No. 07–214, 2007 US Dist. LEXIS 84169 (M.D. Fla. 14 Nov. 2007).
[47] *Viacom International, Inc. v. Admiral Ins. Co.*, No. L-1739-99 (N.J. Super. Ct. App. Div. 21 Apr. 2006) (reprinted in 19–9 Mealey's Poll. Liab. Rep. 21 (2006)).
[48] *Ibid.*
[49] *Ibid.*
[50] *Wasa International Insurance Co Ltd v. Lexington Insurance Co* [2009] Lloyd's Rep. I.R. 675, reversing [2008] Lloyd's Rep. I.R. 510.
[51] *DR Insurance v. Seguros America Banamex* [1993] 1 Lloyd's Rep. 120. Cf. *Agnew v. Lansforsakringsbolagens AB* [2003] Lloyd's Rep. I.R. 637.
[52] *Delver v. Barnes* (1807) 1 Taunt. 48; *Mackenzie v. Whitworth* (1875) 1 Ex. D. 36; *Uzielli v. Boston Marine* (1884) 15 Q.B.D. 11; *British Dominions General v. Duder* [1925] A.C. 639; *Forsikringsaktieselskapet National v. Attorney General* [1925] A.C. 639; *Toomey v. Eagle Star* [1994] 1 Lloyd's Rep. 516; *CNA International Reinsurance Co Ltd v. Companhia de Seguros Tranquilidade SA* [1999] Lloyd's Rep. I.R. 289; *CGU International Insurance Plc v. AstraZenica Insurance Co Ltd* [2006] Lloyd's Rep. I.R. 409; *Zurich Insurance Plc UK Branch v. International Energy Group Ltd* [2015] UKSC 33 for a statement by Lord Sumption that reinsurance is not liability insurance.
[53] *Charter Reinsurance Co Ltd v. Fagan* [1996] 3 All E.R. 46; *Enterprise Oil Ltd v. Strand Insurance Co Ltd* [2007] Lloyd's Rep. I.R. 186. Section 9(1) of the Marine Insurance Act 1906, simply refers to the reinsured reinsuring the risk.
[54] *Wasa International Insurance Co Ltd v. Lexington Insurance Co* [2008] Lloyd's Rep. I.R. 510, reversed [2009] Lloyd's Rep. I.R. 675.
[55] Merkin, *supra* n. 32, para. 20–055.

damage to fixed off-shore drilling, production and accommodation facilities; 'operator's extra expense' (OEE), a type of policy offered to oil and gas companies that provides coverage for expenses associated with regaining control of a well and removing or cleaning up seepage/pollution; 'environmental/pollution liability' which provides coverage for bodily injury, property damage and clean-up costs as a result of a pollution incident; 'business interruption/loss of production income' which provides coverage for energy businesses against loss due to temporary interruption in oil and gas supply from an offshore facility; CGL which provides coverage for claims an energy business is legally obligated to pay as a result of bodily injury or property damage to a third party; 'worker's compensation/employer's liability' providing coverage for claims arising out of employee injuries or deaths incurred while employees are in the line of duty.

As offshore facilities will usually obtain property damage coverage and add casualty coverage for covering clean-up and third-party liability, often one limit will be used for the whole insurance policy, thus creating a challenge for the compensation of third-party liability. Caps in liability may also prove dysfunctional in that they may not allow the allocation of the true sum corresponding to the damage caused by operators in the case of a major oil incident. However, caps in liability sums allow a better and more pragmatic operation of the market. Whilst policy makers can rely on insurance, together with self-insurance, as the most important instrument to cover off-shore related risks, at the same time they need to realize the limitations imposed in terms of available insurance coverage. Post DWH, discussions have indicated what most insurers confirm, i.e. that the available offshore insurance coverage in the market is around USD 500 million to USD 1.5 billion. However, the estimation of the available coverage by insurers may not necessarily reflect a realistic indication of the future available coverage.[56]

4.1 Policy options and considerations

In the aftermath of major oil accidents, such as the DWH, it is crucial to consider potential ramifications including the willingness of the global offshore energy insurance market to participate in the efforts to establish and fix a new liability limit for environmental pollution liability insurance. Such a new limit of liability will have to be supported by the availability of insurance coverage on adequate terms and conditions in the global commercial insurance market given the vulnerability of the insurability of future off-shore oil spill hazards.

Faure and Wang state that as a major source of post-disaster recovery financing, commercial insurance companies have been forced to compensate for catastrophe-related losses, even beyond their contractual policy obligation, such as post 9/11 or in the aftermath of the occurrence of Hurricane Katrina. The off-shore energy insurance underwriters have reassessed their risk exposures in response to newly perceived operational risks involving blowouts, fires, explosions, lost control of well and other non-hurricane risks and have accordingly increased the limit of liability required, whilst at the same time prioritising 'OEE' and 'excess liabilities' coverage and not imposing extra high premiums, in an effort to break the post DWH established cycle of a 'hard' energy insurance market with scarcity of coverage and extremely high premiums prices. In addition, many insurance market experts supported the use of pre-disaster risk financing mechanisms via the use of 'reinsurance sidecars', catastrophe bonds ('CAT bonds') or energy insurance financial futures and options so as to enable the managing and financing large-scale oil spill disasters.[57]

5 Cyber-Risks and the Provision of Cyber-Insurance Coverage

Together with the growth of both the information and communication technology (ICT) and of the impact of cyber-risks to the real-world business, increases the demand for cyber-insurance.[58]

Traditionally cyber cover was mainly embedded in other insurance products, such as business interruption or professional liability insurance, but nowadays such policies tend to exclude the cyber-related risks, due to the complexity of such cyber risk and the potentially catastrophic consequences.[59] As a result, standalone cyber-insurance policies have emerged, however the gap still exists between insurers and assured, in relation to the various differences and exclusions which exist between standalone cyber-insurance contracts and traditional products. In addition, the severity or frequency of cyber-events and the complexity of cyber risks, makes some of these losses insurable and others not.[60]

However, insurers are able to provide coverage and indemnity for third-party liabilities related to certain security events occurring within an organization's IT network, for the costs arising from the damage of data or software – such as the costs relating to recovering or reconstituting the damaged data,[61] as well as for costs relating to extortion in the cyberspace, i.e. in this case in

[56] M. Faure & H. Wang, *The Use of Financial Market Instruments to Cover Liability Following a Major Offshore Accident*, in *Civil Liability and Financial Security for Offshore Oil and Gas Activities* 236–265, 238 (M. Faure ed., 2016).
[57] Faure & Wang, *supra* n. 56, 236–265 at 238.
[58] Petratos, Sandberg & Zhou, *supra* n. 6, 809–836 at 826–27; Marsh, *supra* n. 7.
[59] C. Siegel, T. Sagalow & P. Serritella, *Cyber-Risk Management: Technical and Insurance Controls for Enterprise-Level Security*, 11(4) Info. Systems Sec. 33–49 (2002); Petratos, Sandberg & Zhou, *supra* n. 6, 809–836 at 813–814.
[60] Marsh, *supra* n. 7.
[61] This is so because insurers are able to require the policy holders to follow necessary procedures of data backup or redundancy; Petratos, Sandberg, Zhou, *supra* n. 6, 809–836 at 813–814.

Environmental Sustainability in the Arctic

terms of cover provided for the cost of handling both the cyber incident *per se* and any related ransom payment.

Cyber risks that are classified either as uninsurable or insurable but with certain constraints that may lead to specific exclusions in coverage, include the risk for reputational losses, i.e. losses directly linked to reputational damage, such as the cost of recovering public image or loss of revenue from existing customers; the risk for network business interruption; the risk for physical asset damage as a result of cyber incidents; the risk for death and bodily injury resulting from certain cyber-related incidents from the use of certain equipment (e.g. medical devices, large-scale industry equipment, driverless cars, etc.).[62] The costs incurred by cyber events can largely be differentiated among first and third party losses. First-party losses relate to expenses the firm incurred as a direct result of the incident. Third-party losses, relate to costs incurred due to private litigation, or fines or fees brought by government agencies. It should be noted that, whilst aggregate rates of cyber events and litigation are more frequent and therefore potentially more expensive to organizations collecting and using personal information, on the other hand, such events cost most firms less than USD 200k, which corresponds to only a fraction of the costs commonly cited, a low percentage of firm revenues, and, in any case, far less than other losses due to fraud, theft, corruption, or bad debt.[63]

5.1 Challenges imposed to the development of the cyber-insurance market

In terms of the challenges faced in relation to the development of the cyber insurance market, the US insurance market is more mature than the European market, most notably the UK one, in terms of its response to cyber risks.[64] According to the European Network and Information Security Agency (ENISA), a number of obstacles to the development of a cyber-insurance market in Europe include the difficulty of estimating the extent of the risk and potential losses and a falsely established perception that the existing insurance products offer these coverages, no matter how fragmented such coverage may be, together with the lack of clarity as to the definition of insurable cyber risks. [65]

Gummow and Devilling argue that the cost to businesses affected by data breaches and other cyber hack incidents can prove crippling, not least due to the post cyber breach costs. Despite the potentially catastrophic threat that cyber breaches pose, a large proportion of businesses do not include in their mitigating efforts a cyber-insurance policy, but instead might opt to accept the risk, whilst others might believe that traditional insurance policies provide coverage.[66]

Middleton and Kazamia cite as general reasons, for the low numbers in cyber-insurance policies, the non-availability of such insurance or the fact that the coverage offered by the types of available products is either insufficient or cost-prohibitive.[67] They go on to argue that in spite of attempts for a clearer definition of cyber-related terms,[68] there seems to be some lack of clarity on the exact meaning of these notions.[69] They conclude that as a result, it is difficult to reach consensus within the insurance market as to the risks that a specialized cyber-insurance policy is expected to be addressing, especially taking into account that the legislation addressing that cyber-crime is often fragmented. Being less developed than the US cyber-insurance market, the European market cannot adapt to more flexible premium adjustment. This has the consequence that businesses are usually faced with uncertainty regarding cyber-insurance coverage, the available coverage, limits and exclusions. In addition, courts have varied widely in their interpretation of coverage provisions for cyber losses. All of which creates uncertainty in the landscape. However, cyber-insurance should aim to become a valuable risk management tool, able to address a big part of the damage in case of a successful attack.[70]

5.1.1 First-party coverage: Are cyber-losses 'physical loss or damage' under traditional principles of property insurance law?

Some property policies expressly exclude cyber coverage and in such cases courts have also held that cyber losses are not covered. Accordingly, courts have held that cyber losses are not covered, in cases where a policy is silent as to whether cyber coverage exists. In *Ward Gen. Ins.*

[62] Petratos, Sandberg & Zhou, *supra* n. 6, 809–836 at 826–827.
[63] S. Romanosky, *Examining the Costs and Causes of Cyber-Incidents*, 2(2) J. Cybersecurity 121–135, 129 (2016)
[64] European Network and Information Security Agency (ENISA), *Incentives and Barriers of the Cyber Insurance Market in Europe*, 1, 4, http://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/incentives-and-barriers-of-the-cyber-insurancemarket-in-europe (accessed 3 Mar. 2020); K. Middleton & M. Kazamia, *Cyber Insurance: Underwriting, Scope of Cover, Benefits and Concerns*, in *The 'Dematerialized' Insurance* 192–199 (P. Marano, I. Rokas & P. Kochenburger eds, Springer 2016).
[65] *Ibid.*
[66] S. Gummow & S. Devilling, *Insurance Coverage for Cyber-Risk Exposures* 1–25, 1–2 (New Appleman On Insurance 2017).
[67] Middleton & Kazamia, *supra* n. 64, 192–199; R. Tendulcar, *Joint Staff Working Paper of the IOSCO Research Department and World Federation of Exchanges Staff Working Paper*, SWP1, 1 (2013).
[68] Such as 'cyber-resilience', 'cyber-security', 'cyber-crime', etc.; Middleton & Kazamia, *supra* n. 59, 192–199.
[69] Middleton & Kazamia, *supra* n. 64, 192–199; European Data Protection Supervisor, *Opinion on the Joint Communication and of the High Representative of the European Union for Foreign Affairs and Security Policy on a 'Cyber Security Strategy of the European Union: An Open, Safe, and Secure Cyberspace', and on the Commission Proposal for a Directive Concerning Measures to Ensure a High Common Level of Network and Information Security Across the Union* 7 (2013), https://secure.edps.europa.eu/EDPSWEB/webdav/shared/Documents/Consultation/Opinions/2013/13-06-14_Cyber_security_EN.pdf (accessed 3 Mar. 2020).
[70] Middleton & Kazamia, *supra* n. 64, 192–199; Gummow & Devilling, *supra* n. 61, 1–25 at 1–2.

Environmental Sustainability in the Arctic

Servs., Inc. v. Employers Fire Ins. Co., [71] the court heavily relied on liability coverage cases interpreting data loss under insuring provisions in CGL policies.

Courts are fragmented in their rulings. In *America Online Inc. v. St. Paul Mercury Ins. Co.*,[72] the court concluded that computer data is not tangible physical property; however, to the extent that the software interfered with the computer's operating system and prevented individuals from using their computers, it constituted loss of use of tangible property. However, in *Cincinnati Ins. Co. v. Professional Data Services, Inc.*,[73] the court concluded that there was no insurance coverage, as loss of software had not resulted in tangible loss of the hardware. The court distinguished *America Online Inc. v. St. Paul Mercury Ins. Co.*,[74] noting that it involved allegations that computers were rendered inoperable as a result of the software at issue.[75] However, some courts have held that a loss of data constitutes physical damage. In *Landmark Am. Ins. Co. v. Gulf Coast Analytical Labs., Inc.*,[76] the court held that loss of data constituted as physical, even if intangible, because it can be observed and altered through human action. In *Am. Guarrantee & Liab. Ins. Co. v. Ingram Micro, Inc.*,[77] the court interpreted physical damage as not being restricted to physical destruction or harm but as including loss of access, loss of use and loss of functionality. The *Am. Guarrantee & Liab. Ins. Co. v. Ingram Micro, Inc.*[78] case, illustrates an important distinction in property insurance cases, as it involved the lost programming information critical to the performance of the computer system at issue.[79] However, in 2016, in the case of *Apache Corp. v. Great American Insurance Co.,*[80] which was a case that required from the Court to construe computer fraud coverage in a crime protection policy, the Fifth Circuit held that losses due to e-mail-based fraud schemes that do not involve actual hacking are not covered by a typical computer provision. In 2018, the US Court of Appeals, Sixth Circuit held contrary on similar facts in *American Tooling Ctr., v. Travelers Cas. & Surety Co. of America*,[81] and found that the plaintiff, American Tooling Ctr., suffered a direct loss by computer fraud.[82] In more recent years, insurers have begun to provide specific insurance coverage for cyber risks via the addition of optional coverage extensions to traditional property insurance policies. Whilst such extensions bring data losses into the scope of coverage, still limitations exist because coverage for cyber losses usually depends on what caused the losses. If the cause is not covered, the data loss will not be covered. In addition, numerous policy exclusions may affect the terms of coverage for cyber losses, as there may be exclusions specific to the cyber endorsement, or elsewhere in the policy, that limit the scope of cyber coverage.[83]

5.1.2 Cyber coverage under a CGL policy

For companies without specific cyber-risk insurance coverage, coverage is sought under a CGL policy, whereby typically the claimant will be alleging that the assured negligently permitted hackers to access its computer systems and data. Coverage A of the CGL policy provides coverage for liability owed to a third-party for an occurrence or a wrongful act resulting in bodily injury or property damage, for which the assured is legally obliged to pay damages. Occurrence is usually defined as an accident which does not include intentional acts. *America Online Inc. v. St. Paul Mercury Ins. Co.*,[84] is one of the leading cases analysing whether cyber losses constituted physical damage. Coverage B of a CGL policy provides coverage for certain cyber-related claims, i.e. for the sums that the assured becomes legally obliged to pay as damages.[85]

5.1.3 War risk coverage or exclusion under cyber insurance coverage?

Most companies today maintain CGL coverage, which protects from financial loss, broadly providing defence and indemnity coverage for claims of bodily injury and property damage. But whether a CGL policy will protect businesses from cyberattacks is not always clear. In addition to it depending largely upon the facts of the case, state courts addressing the issue have been inconsistent. While some courts in the US have found that coverage exists (*Travelers Indem. Co. of Am. v. Portal Healthcare Solutions, LLC*[86]*; Eyeblaster, Inc. v. Federal Ins. Co.*[87]) others have denied claims for data breach under CGL

[71] *Ward Gen. Ins. Servs., Inc. v. Employers Fire Ins. Co.*, 114 Cal. App. 4th 548,550, 7 Cal. Rptr. 3d 844, 846 (2003).
[72] *America Online Inc. v. St. Paul Mercury Ins. Co.*, 207 F. Supp. 2d 459, 468–469 (E.D. Va. 2002).
[73] *Cincinnati Ins. Co. v. Professional Data Services, Inc.*,2003 US Dist. LEXIS 15859 (D. Kan. 18 July 2003).
[74] *America Online Inc. v. St. Paul Mercury Ins. Co.*, 207 F. Supp. 2d 459, 468–469 (E.D. Va. 2002).
[75] Gummow & Devilling, *supra* n. 66, 1–25 at 3–4.
[76] *Landmark Am. Ins. Co. v. Gulf Coast Analytical Labs., Inc.*, 2012 US Dist. LEXIS 45184 (M.D. La. 30 Mar. 2012).
[77] *Am. Guarrantee & Liab. Ins. Co. v. Ingram Micro, Inc.*, 2000 US Dist. LEXIS 7299 (D. Ariz. 18 Apr. 2000).
[78] *Ibid.*
[79] Gummow & Devilling, *supra* n. 66, 1–25 at 3–5.
[80] *Apache Corp. v. Great Am. Ins. Co.*, 2016 WL 6090901 (5th Cir. Oct. 18 2016); *See also Great Am. Ins. Co. v. AFS/IBEX Fin. Servs., Inc.*, CIV. A. 307-CV-924-O, 2008 WL 2795205 (N. D. Tex. 21 July 2008), aff'd. 612 F. 3d 800 (5th Cir. 2010).
[81] *American Tooling Ctr., v. Travelers Cas. & Sur. Co. of America*, US Court of Appeals (6th Cir. 13 July 2018).
[82] A. Johnson, *Twenty-first Century Insurance: Cyber Insurance*, (8) Computer & Internet Law. 4–25, 4–5 (2019).
[83] *GTE Corp. v. Allendate Mut. Ins. Co.*, 372F.3d. 598, 601 (3d Cir. 2004).
[84] *America Online Inc. v. St. Paul Mercury Ins. Co.*, 207 F. Supp. 2d 459, 468–469 (E.D. Va. 2002).
[85] *Recall Total Information Management, Inc. v. Federal Ins. Co.*, 147 Conn. App. 450, 83 A.3d 664 (2014); Gummow & Devilling, *supra* n. 61, 1–25 at 11–14.
[86] *Travelers Indem. Co. of Am. v. Portal Healthcare Solutions, LLC,* 644 Fed. Appx. 245 (4th Cir. 2016).
[87] *Eyeblaster, Inc. v. Federal Ins. Co.*, 613 F.3d 797 (8th Cir. 2010)).

Environmental Sustainability in the Arctic

policies (*Zurich American Insurance Co. v. Sony Corp. of America*[88]; *Recall Total Info. Mgmt. v. Fed. Ins. Co.).*[89]

Given this jurisdictional uncertainty and the fact that the standard CGL ISO policy form and many CGL polices in general have been amended in recent years to contain exclusions for breaches from cyberattacks, many companies have fittingly turned to specific cyber liability coverage to fill the gaps, including special war risk coverage. Cyber liability policies typically cover a variety of liability and property losses or some combination of traditional liability coverage protecting against claims by third parties, and first-party coverage protecting against losses suffered by the insured. However, cyber policies often feature various broadly worded exclusions that can limit or preclude coverage. Some commentators have suggested that the so-called war risk exclusion might be a viable means for insurers to exclude coverage for cyber risks. Both CGL policies and cyber liability policies generally exclude coverage for 'acts of war' or 'warlike activity'. Whether or not a particular cyberattack or data breach is considered an act of war is critical to whether the exclusion applies. The problem is that there is no universal definition of war, let alone agreement on what constitutes an act of war in the cyber context. Different government entities and different insurance carriers define war in different ways. And while the language in CGL policies is more uniform, there is no standard form on which the insurance industry as a whole underwrites cyber coverage. Cyber insurance is still in its relative infancy, and the language contained in cyber policies thus tends to vary significantly.

In addition, insurers always have the burden to prove an exclusion application. The war risk exclusion presents insurers with a particularly formidable evidentiary challenge in the cyber context. Courts have traditionally interpreted the war exclusion narrowly, defining 'war' as a physical event involving two sovereigns or quasi-sovereign governmental entities. Thus, without direct involvement by a sovereign state, the war exclusion would generally not bar coverage.[90]

In the immediate aftermath of the 11 September 2001 attacks, there was intense political pressure on the insurance industry not to invoke the 'war risk' exclusion contained in any responsible party's liability policy, and the consensus depicted among some insurance commentators was that the 'war risk' exclusion was inapplicable anyway. Such a conclusion was generally based on the Second Circuit's 1974 decision in *Pan American World Airways v. Aetna Casualty and Surety Co.*[91] where the Court of Appeals held that a war risk exclusion did not preclude coverage for the hijacking and destruction of an airplane by the Popular Front for the Liberation of Palestine. The court's rationale was that English and American cases dealing with the insurance meaning of 'war' have defined it in accordance with the ancient international law definition stating that war refers to and includes only hostilities carried on by entities that constitute governments or entities that have at least significant attributes of sovereignty. Applying the above rationale to *Pan American World Airways v. Aetna Casualty and Surety Co.*,[92] the court held that the loss of the Pan American 747 was in no sense proximately caused by any 'war' as the latter is to be defined. This 'war risk' exclusion was likewise adopted to the events of September 11th even if in the end the insurers did not invoke the 'war risk' exclusion and going forward the focus turned to the insurability of losses arising out of terrorist attacks. However, in *In re September 11 Litigation*,[93] the issue was whether the 'act of war' exception to CERCLA liability constituted a defence to the plaintiff's claims, the court held that it did, addressing also *Pan American World Airways v. Aetna Casualty and Surety Co.*[94] and deciding that it was distinguishable and expressing its unwillingness to treat 'war' as a static concept.[95]

The nature of cyber incidents is problematic for insurers.[96] Although any insurer seeking to rely on the war exclusion to preclude coverage for cyber risks faces an uphill climb, it is nevertheless important for policyholders to be mindful of applicable policy terms, conditions, and exclusions. All exclusions are not created equally and because there is no definitive answer, as to when a cyberattack may be considered an act of war thereby excluding coverage, companies should in an abundance of caution resist the inclusion of such boilerplate exclusions, and, instead, negotiate the specific inclusion of cyberwar and terrorism coverage to ensure that a broad range of events will be covered regardless of motive or origin.[97]

5.2 Globalization and security challenges arising from cyber-attacks: policy options

Globalization and technological evolutions are forcing drastic changes in our lives. While the internet and new technologies (Internet of Things (IoT), Artificial

[88] *Zurich American Insurance Co. v. Sony Corp. of America*, No. 651982/2011 (N.Y. Sup. Ct. 24 Feb. 2014).
[89] *Recall Total Info. Mgmt. v. Fed. Ins. Co.*, 147 Conn. App. 450 (Conn. App. Ct. 2014.
[90] *Pan Am. World Airways, Inc. v. Aetna Cas. & Surety Co.*, 505 F.2d 989 (2d Cir. 1974).
[91] *Ibid.*
[92] *Ibid.*
[93] *In re Sept. 11 Litig.*, 931 F. Supp. 2d 496, 511 (S.D.N.Y. 2013).
[94] *Pan Am. World Airways, Inc. v. Aetna Cas. & Surety Co.*, 505 F.2d 989 (2d Cir. 1974).
[95] R. J. Maniloff, *Coverage Opinions – September 11th: Revisiting The 'War Risk' Exclusion*, White and Williams, LLP, https://www.lexisnexis.com/legalnewsroom/insurance/b/exclusions/posts/coverage-opinions-september-11th-revisiting-the-war-risk-exclusion (accessed 3 Mar. 2020).
[96] *In re Sept. 11 Litig.*, 931 F. Supp. 2d 496, 511 (S.D.N.Y. 2013) loosening the act of war exclusion to extend to claims arising out of 9/11 and distinguishing the *Pan Am. World Airways, Inc. v. Aetna Cas. & Surety Co.*, 505 F.2d 989 (2d Cir. 1974) precedent requiring a state actor to conduct war.
[97] K. R. Doherty, *The Art of (Cyber) War*, 29(6) Intell. Prop. & Tech. L. J. (2017).

Intelligence (AI)) have connected people like never before, technological advances come with many inherent challenges, such as cyber-attacks.

Policy recommendations to address cyber-attacks include the continuation of investment in resources so as to combat such cyber threats. In addition to funding the existing programs, governments need collaborate with private companies so as to train their personnel so as to be able to address cyber-attack challenges. Also, governments should continue to promote cybersecurity programs through other additional mechanisms (e.g. more grant money to fund cybersecurity research).[98]

Big or small scale cyber or war risk attacks, the challenge for insurers will likely be that, as with September 11th, demands will be made on them to provide immediate answers to coverage questions. As *In re September 11 Litigation*[99] demonstrates, the facts that will determine coverage under the circumstances will not likely be immediately available, and, for that matter, may not be available for significant periods of time. [100]

6 Cyber Threats in the Energy Sector: Insurance as a Mechanism to Address Cyber Risks in Oil and Gas Installations

In the energy sector, oil and gas companies face unique cyber risks which make cyber-security even more challenging and calls for separate cyber insurance, usually appearing as first-party coverage (data loss, business interruption, network failure and other cyber losses) or as third-party coverage (liability and defence cost insurance for claims brought by third parties).

A frequently encountered problem in insurances for oil and gas cyber-attacks is the fact that although such attacks pose a risk of environmental liability, cyber insurance policies may limit or bar coverage entirely for claims involving the release of pollutants, for which the industry faces significant exposures and whereby broadly worded liability policies will often contain exclusions barring coverage for any loss arising from cyber events. This entails that policyholders will need to look for insurance update or revisions to maintain adequate coverage in place and to regularly negotiate and amend policies so as to be able to address any specific cyber risks that may surface.[101]

Coverage issues for cyber risks are usually exemplified in a lack of awareness about the availability of specific coverage and a lack in the harmonization of the policy language and conditions.[102] Moreover, in relation to the Arctic, the increased exposure to environmental threats and climate change forge the need to protect critical infrastructure. For the effective management of cyber threats, both the public and private sectors should be involved in managing the interests of stakeholders. Not least, because at the international, EU and national levels, there is a lack of legal uniformity for the protection of critical infrastructure, insurance can play a mitigating role.[103]

However, the provision of such insurance coverage can prove to be problematic because there is a difficulty in understanding cyber risk both from the insurer's and the policyholder's point of view, as the policyholder may not understand the products or their own needs, whilst the insurer may not be able to assess the risk due to a lack of data, or due to a systemic nature of major potential events. All of this may result in difficulties to understand the dimension and the accumulated risks for the market as a whole, lead the insurers towards writing cyber risk on the least possible amount of information, and result in underpriced risk covers. In addition, the insurance market faces substantial difficulties in properly quantifying and funding the risks involved as a result of the increase in the connectivity of destructive attacks and of the potential subsequent aggregation risk.

Overall, of the key concerns raised by insurers in their effort for a deeper understanding of cyber risk is the broadness of coverage, terms and conditions, the difficulties in properly quantifying risks, the risk of under-pricing, the lack of appropriate reinsurance coverage, the improper address of silent risks, the lack of historical data, the insufficient information on risks, the systemic nature of potential events and the lack of specialized underwriters.

As a result, even if the cyber insurance industry is growing, the insurance risks are not fully understood, due to the scarcity or lack of sufficient amounts of claims data, the difficulty in measuring the relevance to the current or the future cyber landscape because of the rapid technological advances, the lack of specialized underwriters, data and quantitative tools, all of which, together with the passing of the proper regulation, could help to address some of the identified challenges and

[98] B. Fonseca & J. Rosen, *Cybersecurity in the US: Major Trends and Challenges*, in *The New US Security Agenda* 57–106 (B. Fonseca & J. Rosen eds, Palgrave Macmillan 2017).
[99] *In re Sept. 11 Litig.*, 931 F. Supp. 2d 496, 511 (S.D.N.Y. 2013).
[100] Fonseca & Rosen, *supra* n. 98, 57–106.
[101] J. Lawrence et al., *Insurance Mitigates Cyber-Related Risk*, The American Oil and Gas Reporter (Dec. 2017), https://www.huntonak.com/images/content/3/4/v2/34783/Insurance-Mitigates-Cyber-Related-Risk.pdf (accessed 3 Mar. 2020).
[102] OECD, *Enhancing the Role of Insurance in Cyber Risk Management* 104–106 (Paris: OECD Publishing, 2017), http://dx.doi.org/10.1787/9789264282148-en, (accessed 3 Mar. 2020).
[103] S. Cassota et al., *Climate Change, Environmental Threats and Cybersecurity in the European High North*, in *Enablement Besides Constraints: Human Security and a Cyber Multi-Disciplinary Framework in the European High North*, 47 Juridica Lapponica 90, 92, 102–103 (G. Zojer ed., Arctic Centre, Lapland – Rovaniemi 2019).

therefore enhance the development of the industry and the provision of proper coverage to the economy.[104]

7 The EU and EU Arctic States Response

The energy sector is experiencing changes at a scale and pace that are unprecedented in more than a century. These are driven by the urgency of actions required to mitigate climate change and formulate a strategy to provide adequate cyber security via the implementation of laws and other legislative or non-legislative recommendations, such as the alignment of cyber security activities across all critical infrastructure; the development of security standards for energy systems or the establishment of a stakeholder network for energy security.[105]

Of the EU/EEA countries closely connected to the Arctic, Denmark, in its strategy for the Arctic 2011–2020 addresses the need in developing the Arctic while appreciating its human impact, i.e. the economic and social integration of the population and with sensitivity to environmental concerns. For the exploration and exploitation of oil and gas resources, as per the Greenland Mineral Resources Act, the licensee must ensure that safety, environmental and health risks are identified, assessed and reduced, and a strategic environmental impact assessment exists to ensure that any oil/gas activities can be implemented on an environmentally sustainable basis.[106] The same applies for Finland which is also committed to the sustainable development in the utilization of the economic growth potential in the Arctic region. In line with comprehensive security thinking, Finland strengthens its capacity to identify wide-ranging hybrid influencing against society, and the capabilities to improve cyber security. [107]

Cyber insurance may be the vehicle towards the enhancement of cybersecurity via the adoption of best practices. This is because insurance providers usually require a level of security or protective measures as a precondition of coverage and offer lower insurance rates to companies adopting adequate security measures. Therefore, the adaptation of best practices, is a vehicle to encourage investments and improvements that further bolster cybersecurity.[108] However, underwriting some cyber exposures can prove to be a difficult task, as they pertain to not only the physical buildings and properties, but also critical engineering, production, distribution, and emergency systems. In addition, the insurance industry may not have the capacity to underwrite some exposures because a number of open questions remain on how one can quantify and underwrite some of these exposures, the threats to systems supporting critical infrastructure are evolving and growing and because reliable indicators of measuring the frequency or the economic impact of cyber-attacks are rarely available. Thus, protecting and insuring these many components of critical infrastructure is a challenging, ongoing task for the insurance industry, as well as for the policymakers.[109] Notwithstanding the above remarks, the insurance industry can still play a critical role as risk manager, underwriter and investor in addressing cyber security risks, which may hinder its' function as a risk mitigation mechanism,[110] however, for such a mitigation mechanism and role for the insurance industry it is absolutely necessary that it be backed up by a robust regulatory environment.

The EU has a high level of energy security including the oil and gas sector. As the production, distribution and use of energy is becoming increasingly digitalized, this provides increased opportunities for malicious actors to carry out attacks on the energy system, notably cyber-attacks. The key EU law for the protection of critical infrastructure is Council Directive 2008/114/EC on critical European infrastructures which establishes procedures for identifying and designating European critical infrastructures (ECI) and introduces a common approach for assessing their protection and the need to improve it, requiring owners or operators of designated ECI to prepare advanced business continuity plans (operator security plans) for critical infrastructure protection. In April 2019 the European Commission issued Recommendation (EU) 2019/553, containing guidelines that Member States and key stakeholders should take into account when making decisions about infrastructure and with protection measures against cyber-attacks. In June 2019, the Commission published an evaluation of Directive 2008/114/EC on critical European infrastructures, which found that

[104] EIOPA, *Understanding Cyber Insurance – A Structured Dialogue with Insurance Companies* (Publications Office of the European Union 2018), https://www.eiopa.europa.eu/sites/default/files/publications/reports/eiopa_understanding_cyber_-insurance.pdf, (accessed 3 Mar. 2020).

[105] D. Healey et al., *Cyber Security Strategy for the Energy Sector*, ITRE, EU (2018), http://www.europarl.europa.eu/studies (accessed 3 Mar. 2020).

[106] Denmark, Greenland and the Faroe Islands, *Kingdom of Denmark Strategy for the Arctic 2011–2020*, Ministry Foreign Aff. (2011), http://library.arcticportal.org/1890/1/DENMARK.pdf (accessed 3 Mar. 2020).

[107] Prime Minister's Office Publications, *Government Report on Finnish Foreign and Security Policy*, (Sept. 2016), https://valtioneuvosto.fi/documents/10616/1986338/VNKJ092016+en.pdf/b33c3703-29f4-4cce-a910-b05e32b676b9 (accessed 3 Mar. 2020).

[108] US Department of Energy, *Insurance as a Risk Management Instrument for Energy Infrastructure Security and Resilience* 39, 41–42 (2013), https://www.energy.gov/sites/prod/files/2013/03/f0/03282013_Final_Insurance_EnergyInfrastructure.pdf (accessed 3 Mar. 2020).

[109] *Ibid.*

[110] M. Golnaraghi, *Climate Change and the Insurance Industry: Taking Action as Risk Managers and Investors Perspectives from C-level executives in the insurance industry* (The Geneva Association 2018), https://www.genevaassociation.org/sites/default/files/research-topics-document type/pdf_public/climate_change_and_the_insurance_industry__taking_action_as_-risk_managers_and_investors.pdf (accessed 3 Mar. 2020).

the Directive's relevance has diminished and that the Directive has failed to establish a common approach to the assessment of critical infrastructure protection measures. In addition, the Cybersecurity Act (Regulation (EU) 2019/881 cybersecurity package) aims to strengthen the EU's response to cyber-attacks, improve cyber-resilience and increase trust in the digital single market.[111]

Adding to the regulatory framework, cyber insurance may be the vehicle towards the enhancement of cybersecurity via the adoption of best practices. This is because insurance providers usually require a level of security or protective measures as a precondition of coverage and offer lower insurance rates to companies adopting adequate security measures. Therefore, the adaptation of best practices is a vehicle to encourage investments and improvements that further bolster cybersecurity.[112] However, underwriting some cyber exposures can prove to be a difficult task, as they pertain to not only the physical buildings and properties, but also critical engineering, production, distribution, and emergency systems. In addition, the insurance industry may not have the capacity to underwrite some exposures because a number of open questions remain on how one can quantify and underwrite some of these exposures, the threats to systems supporting critical infrastructure are evolving and growing and because reliable indicators of measuring the frequency or the economic impact of cyber-attacks are rarely available. Thus, protecting and insuring these many components of critical infrastructure is a challenging, ongoing task for the insurance industry, as well as for the policymakers.[113] The insurance industry can play a critical role as risk manager, underwriter and investor in addressing climate change goals, targets and key barriers that hinder its' function as a risk mitigation mechanism.[114]

Advances in communications and technology encompass inherent challenges, such as the threat of cyberterrorism. Accordingly, cybersecurity has been elevated to one of the most important national security threats on the security agenda of many countries.[117] It has also been argued that a catastrophic cyber event could bring major losses to Lloyd's reinsurers, as reinsurers could be exposed to the full limits on policies that were originally intended to cover property damage or casualty lines in case a cyber 'hack' is found to be the proximate cause of loss.[118]

Case law is evolving rapidly in relation to cyber issues, although it appears to have a fragmented approach. Policy language is critical to the evaluation of cyber-related claims, particularly win relation to non-cyber policies, and given the growing tendency of insurers to revise policies so as to address cyber-risk.[119]

It has been stated also that because on the one hand, cyber-attacks can be epidemic and because on the other hand, there is limited coverage for cyber liability under general commercial policies, any cybersecurity policy should be a primary policy, so as to be able to respond first.[120] Given such a volatile legal landscape, the assureds need to thoroughly examine their existing cyber coverage and any applicable exclusions. Insurers need also understand that many courts have stretched traditional coverage principles to find coverage for cyber losses under policy provisions traditionally applicable to physical losses.[121]

Finally, as reiterated also by Curran, Connolly and O' Driscoll, it is essential to comprehend that, notwithstanding the rapid growth of the cybersecurity industry, it is still an industry in its infancy, with new insurance products and often limited coverage. It is imperative that all companies try to mitigate the threats imposed by the potential of a cyber-security incident in the energy sector, and, hence, identify potential additional risks and try to

8 Conclusion

As climate change accelerates, ice melts in the Arctic faster than ever before and poses the Arctic energy scene in the forefront due to the oil and gas potential entailed.[115]

It has been argued that the global oil and gas industry needs make firm commitments for the sustainable development of oil and gas in the Arctic, as the prospect of expropriation in it of yet non-explored reserves is close to realization.[116] Hence, there is an imminent need for measures to help protect the Arctic environment and mitigate any potential harm. Insurance for environmental and cyber-incidents from the expropriation of oil and gas in the Arctic is indispensably needed and linked to this new prospect of financial activity in the area. Such insurance coverage needs to be specifically worded and underwritten so as to cover the gradual character of occurrence of environmental harm as far as the environmental liability coverage is concerned, given the feature of 'sudden' and 'unexpected' loss coverage which is usually found in property casualty policies, and at the same time provide adequate coverage for cybersecurity occurrences.

[111] G. Erbach & J. O'Shea, *Cybersecurity of Critical Energy Infrastructure* (European Parliamentary Research Service (EPRS) Oct. 2019), https://www.europarl.europa.eu/RegData/etudes/BRIE/2019/642274/EPRS_BRI(2019)642274_EN.pdf, (accessed 3 Mar. 2020).
[112] US Department of Energy, *supra* n. 108, at 41–42.
[113] *Ibid.*
[114] Golnaraghi, *supra* n. 110.
[115] Surveys conducted are persistently and frequently showing repeated figures of 30% of the world's yet-to-find (or undiscovered) gas reserves and of 13% of the undiscovered oil reserves (circa forty-seven trillion cubic metres of gas and ninety billion barrels of oil) available to be explored in the Arctic region.
[116] C. Nakhle, *The Arctic: The Last Great Oil Frontier – Or Is It*?, (6) I.E.L.R. 173 (2010).
[117] Gummow & Devilling, *supra* n. 66, 1–25 at 21.
[118] V. Beckett, *Cyber Cat May Bring Big Lloyd's Losses* (18 July 2016), http://www.euromoneyseminars.com/articles/3571301/cyber-cat-may-bring-big-lloyds-losses.html (accessed 3 Mar. 2020).
[119] Gummow & Devilling, *supra* n. 66, 1–25 at 21.
[120] Johnson, *supra* n. 82, 4–25 at 20.
[121] Gummow & Devilling, *supra* n. 66, 1–25 at 21.

Environmental Sustainability in the Arctic

have them minimized and transferred externally. One way of doing so is via cybersecurity insurance. As cybersecurity breaches and threats, such as the Saudi Aramco attack in 2012 or the latest drone attack in Saudi Aramco's plants in September 2019, continue to hit headlines worldwide, taking out a cybersecurity policy should be as obvious as taking out any other type commercial general liability insurance.[122]

It follows from the above that the globalization of environmental risk is more intense than ever before nowadays, not least because of the challenges that the threat of potential cyber-risks occurrences have imposed. Although the civil liability regime for marine and oil pollution has extended the scope of compensation obligations to include environmental impairment – nevertheless and given that vulnerability to cyber-attacks increases – cyber insurance for risks related to malicious cyber-attacks on the infrastructure of oil and gas installations is an imperative insurance coverage element that all players in the field should have, as the Saudi Aramco incidents have revealed.

As argued in this article, the usually encountered 'sudden' and 'unexpected' loss coverage in property casualty policies, is not appropriate for environmental pollution coverage which by definition and nature is usually gradually occurring. Often, natural resources expropriation companies obtain property damage coverage and add casualty coverage for covering clean-up and third-party liability. It is notable that the DWH incident which was dramatic both in nature and in extent, led to the establishment of a 'hard' energy insurance market with scarcity of coverage and high premiums. However, the threat and frequency of cyber-risks have provided the need for specific and separate additional coverage for cyber terrorism and cyber risks. This in turn has been anticipated to re-establish a 'soft' hence more pragmatic and accessible energy insurance market, medium and long-term.

[122] D. Curran, B. Connolly & F. O' Driscoll, *Cybersecurity Insurance: Transferring the Risk*, 6(3) Comp. & Risk 13 (2017).